www.ict4peace.org

International Cyber Security Capacity Building Program

Promoting Openness, Prosperity, Trust and Security in Cyberspace

States bear primary responsibility for the safety and security of their citizens, including in the ICT environment. Many states, especially developing countries and LDCs however, still lack sufficient capacity to protect their ICT networks and to engage in bilateral, regional and global cooperation at the technical and diplomatic level and to learn about concrete threats and respond effectively to them.

The lack of such capacity can make national institutions, critical infrastructures such as power, Telecom, hospitals, transport and financial sector of a country or the citizens and the private sector at large vulnerable and can hamper economic and social development. It can make a country even an unwitting haven for malicious actors, which negatively impacts the global ICT network on the whole, thus also in the industrial world. It is often said, that the global ICT network "is only as strong as its weakest link".

Support to capacity building in cyber security policy, strategy and diplomacy is playing an essential role in (1) States engaging in international cooperation and negotiations (as outlined in the 2013 and 2015 GGE reports on norms and CBMs), (2) enabling countries to secure its ICT infrastructure for economic and social development and (3) to strengthen the global ICT network and to ensure their peaceful use for economic and social development.

Since 2014 and with the support of the Governments of the UK, Germany, Switzerland, Netherlands, Colombia, Kenya, Singapore, Australia and New Zealand, the ICT4Peace Foundation has carried out a series of Capacity Building workshops for Latin American Countries (in Bogota in cooperation with OAS), for African Countries (AU, Addis Ababa), for East African Countries (Nairobi), for ASEAN Countries (Singapore), Europe (GCSP, Geneva), for OSCE Field staff (Vienna), for Cambodia, Laos, Myanmar, Vietnam (CLMV countries) in Laos, Vientiane; Hanoi, Vietnam, for ASEAN Countries Thailand and in Singapore. A further workshop for CLMV Countries is planned for May 2018 in Cambodia.

We cooperate with the UN GGE and OEWG experts on refining and delivering the next round of workshops to support the goals and tasks outlined in the GGE reports and the specific needs of the countries in the Regions.

General Objectives of the Workshops

1. Better awareness of issues of international cyber security by public officials and diplomats (international law and norms, CBMs and international cooperation as outlined in the UN GGE Reports, by ASEAN, OSCE, AU, OAS etc.);
2. Preparation of staff in Capitals and Country Delegations for the upcoming negotiations on Cybersecurity in the context of the OEWG and UN GGE in 2019 in New York.
3. Feedback from the Regions to the international cyber security dialogue and discourse;
4. Better mutual understanding of related concepts, norms and measures, strengthened and possibly institutionalized cooperation among participating countries;
5. Exchange of concerns, best practices, policies and institutional arrangements in the field of cyber security;
6. A network of alumni, lecturers and experts familiar with the international cyber security challenges and processes and willing to support the goals of implementing and universally promoting inter alia the UN GGE guidance on norms and CBMs.

Workshop Modules

1. Introduction to the international peace and security goals related to uses of ICTs;
2. Links between national and international cyber security efforts, processes and actors;
3. Introduction to international cyber security consultations and dialogues (UN GGE, ASEAN, ARF, OSCE, AU, OAS, London Process etc.);
4. Applicability of the international law as outlined in the UN GGE reports;
5. Norms of responsible state behavior as outlined in the UN GGE reports;
6. CBMs and international cooperation in the cyberspace (as outlined in the UN GGE, OSCE, ARF etc. reports);
7. Best practices in national cyber security strategy building, policy development and legislation;
8. Best practices in Cert building and Cert-Cert cooperation;
9. Presentations and panel discussions on regional and national cyber security concerns, perspectives and policy options;
10. Table-top exercises to assess national cybersecurity resilience and identify gap.
11. Table-top exercises tailored to the target audience priorities and requirements.

Additional courses and seminars upon request

1. Workshops and consultations on best practices of National Cyber Security Strategy (NCSS) building;
2. Workshops and consultations on developing and implementing national legislation;
3. Workshops on establishing CERTs, CERT- CERT cooperation;
4. Workshops for special target audiences (parliamentarians, judiciary, regulatory authorities etc.)

Participation

These workshops will be of particular interest to government officials involved or interested in foreign cyber policy development and/or cyber security diplomacy but offer useful background knowledge to decision-makers and advisers in the field of national cyber security strategy development and implementation. Senior staff of technical cybersecurity units such as CERTs and the Private Sector will be included wherever possible.

A ceiling of approximately 35 participants per workshop is recommended to facilitate discussion.

Lecturers and facilitators of the workshop

The lecturers and facilitators of the workshop consist of senior experts and diplomats having participated in the processes of UN GGE, OSCE or ARF CBMs, and senior experts with civil society/academic background and first-hand experience with the topic.

Links to Workshops already carried out on International Law, Norms and CBMs, CERT-Building, Strategy building and Legislation etc. :

2014 Bogota with OAS: http://ict4peace.org/?p=3563 and http://ict4peace.org/?p=3693
2015 The Hague Global Conference on Cyberspace 2015 http://ict4peace.org/?p=3693
2015 Kenya for 12 East African countries: http://ict4peace.org/?p=3674
2015 Singapore for ASEAN Countries: http://ict4peace.org/?p=3969
2016 Addis Ababa with AU Commission: http://ict4peace.org/?p=4079
2016 Vientiane for CLMV Countries: http://ict4peace.org/?p=4304
2016 GCSP, Geneva based diplomats, business and civil society: http://ict4peace.org/?p=4095
2016 Vienna for OSCE field staff: http://ict4peace.org/?p=4781
2016 Bangkok Regional Workshop for ASEAN countries: http://ict4peace.org/?p=4849
2017 UN Geneva: for the UN GGE Experts: Existing and Future Norms on International ICT Infrastructure and Data Integrity: http://ict4peace.org/?p=4804

2017 Singapore for ASEAN Countries: http://ict4peace.org/?p=4901
2017 Hanoi for CLMV Countries http://ict4peace.org/?p=5095
2018 Brunei for ASEAN Countries: http://ict4peace.org/?p=5285
2018 Singapore 2nd ASEAN Cyber Norms https://ict4peace.org/activities/2nd-asean-cyber-norms-workshop-in-singapore-supported-by-ict4peace/
2018 Siem Reap for CLMV Countries
https://ict4peace.org/activities/capacity-building/capacity-building-cs/ict4peace-3rd-senior-level-cybersecurity-policy-and-diplomacy-workshop-for-clmv-countries-held-in-siem-reap-cambodia/
2019 Naypyitaw (Myanmar) for CLMV Countries:
https://ict4peace.org/activities/capacity-building/capacity-building-cs/4th-ict4peace-senior-level-cybersecurity-policy-and-diplomacy-workshop-for-clmv-countries-held-in-naypyitaw-myanmar/

Links to selected list of ICT4Peace publications:

Getting Down to Business: Realistic Goals for the Promotion of Peace in Cyber-Space (2011)
Developments in the Field of Information and Telecommunication in the Context of International Security (2012)
Cyber Security Affairs: Global and Regional Processes, Agendas and Instruments (2013)
Confidence Building Measures and International Cyber Security (2013)
A Role for Civil Society? ICTs, Norms and Confidence Building Measures in the Context of International Security (2014)
Baseline Review of ICT-Related Processes and Events (2014)
Voluntary, Non-Binding, Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary (Published by UNODA, New York) (2017)
UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes (2019)

For additional information, cooperation or other requests please contact:

Dr. Daniel Stauffacher
President
ICT4Peace Foundation
danielstauffacher@ict4peace.org

Geneva, 11 July 2019